Eerste Kamer der Staten-Generaal 1

Vergaderjaar 2014–2015

CVIII Rol van de overheid bij digitale dataverwerking en -uitwisseling II; privacy en toezicht op de inlichtingen- en veiligheidsdiensten

Q BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 25 maart 2015

Bij het debat over de rol van de overheid bij digitale dataverwerking en -uitwisseling II, op 23 september 2014, heb ik naar aanleiding van vragen van Kamerlid Duthler de toezegging gedaan om de Kamer te informeren over de voortgang bij het verbeteren van en het ontwikkelen van alternatieven voor DigiD. In de motie van het lid Duthler c.s. van 7 oktober 2014 is gevraagd om uw Kamer hierover voor het einde van het jaar te informeren.

Vanwege de samenhang tussen de ontwikkeling van alternatieven voor DigiD en de ontwikkeling van het eID Stelsel heeft de voorbereiding van het gevraagde overzicht enige extra tijd gekost. Mede omdat over zowel de verbetering van DigiD als het eID Stelsel in de afgelopen maand een brief aan de Tweede Kamer is gezonden, respectievelijk op 24 en 9 februari jl.[1]

In deze brief krijgt u een actueel overzicht van de voortgang op beide onderwerpen.

Introductie DigiD

Op dit moment kent DigiD de niveaus Basis en Midden. Voor Basis identificeren gebruikers zich met een gebruikersnaam en een wachtwoord; voor Midden identificeren gebruikers zich met een gebruikersnaam, een wachtwoord én een SMS-code.

[1] Tweede Kamer, jaarvergadering 2014–2015, 26 643, nrs. 349 en 352

kst-CVIII-Q
ISSN 0921 - 7371
’s-Gravenhage 2015

DigiD Basis en DigiD Midden zijn van STORK niveau 2 resp. 2+.[2] Het voordeel van DigiD Midden boven DigiD Basis is dat daarmee in belangrijke mate wordt voorkomen dat burgers hun accountgegevens onbewust afstaan en dat daarmee het risico van «phishing» van accountgegevens kan worden tegengegaan. Deze praktijken behoren tot de grootste problemen binnen en buiten overheid bij voorkomen van fraude en oneigenlijk gebruik bij digitale dienstverlening.

Om DigiD op STORK niveau 3 te krijgen is face to face uitgifte van de accounts nodig; dat zou bijvoorbeeld kunnen via thuisbezorging of balie-uitgifte van activeringscodes. Deze methoden worden momenteel op beperkte schaal toegepast. Het thuisbezorgen vindt plaats in bepaalde postcode gebieden met een verhoogd risico en DigiD buitenland kent een vorm van balie-uitgifte. Het hoogste betrouwbaarheidsniveau (STORK 4) is nog niet beschikbaar; om dat niveau te halen, dient gebruik te worden gemaakt van gekwalificeerde elektronische certificaten.
DigiD heeft op dit moment ca. 600 aangesloten afnemers en kent ca. 11 miljoen gebruikers. Deze genereerden in 2014 ca. 158 miljoen authenticaties. De beschikbaarheid voor DigiD lag in 2014 boven de met de leveranciers afgesproken norm van 99,95%.

Deze cijfers geven duidelijk het belang weer van DigiD. Het is belangrijk om met vereende kracht het hoofd te blijven bieden aan de steeds toenemende dreigingen voor de betrouwbaarheid en de continuïteit van een goede en veilige elektronische toegang tot de overheid. Om deze dienstverlening veilig te houden en tegelijk ook toekomstbestendig te maken, zijn en worden permanent de nodige inspanningen verricht.

Dienstaanbieders kiezen wel zelf het zekerheidsniveau dat bij hun diensten past. Op 31 oktober 2014 heb ik alle DigiD gebruikende organisatie gewezen op de nieuwe versie van de Handreiking Betrouwbaarheidsniveaus van het Forum Standaardisatie die hen handvatten hiervoor biedt. Dienstaanbieders kunnen ervoor kiezen om voor één of meer diensten en/of producten DigiD Midden in te zetten. Zo is bijvoorbeeld bij de Dienst Uitvoering Onderwijs inloggen alleen mogelijk met DigiD Midden.

Bij het digitaal aanbieden van diensten en producten is het overheidsinstellingen er veel aan gelegen dat zowel veilig als klantvriendelijk te doen: zij trachten de drempel voor het gebruik – en daarmee de uitvoeringskosten – zo laag mogelijk te houden en tegelijk het risico op misbruik en/of oneigenlijk gebruik zo veel mogelijk te vermijden. Naast het voorkomen van schade hebben het imago van en het vertrouwen in DigiD hun onverdeelde aandacht. Maatregelen worden geselecteerd in overeenstemming met risico en belang. Aanvullend aan het gebruik van DigiD worden door de dienstaanbieders mitigerende maatregelen getroffen om misbruik en oneigenlijk gebruik te voorkomen, zoals bij het wijzigen van adresgegevens of bankrekeningnummers.

[2] STORK is een Europese classificatie die vier betrouwbaarheidsniveaus voor elektronische identificatie onderkent. Niveau 4 is het hoogste betrouwbaarheidsniveau en geeft aan dat de identiteit van de gebruiker met zeer grote zekerheid is vastgesteld. Eind juni 2015 wordt in het eIDAS comité besloten over een andere classificatie die beter aansluit bij de aankomende Europese verordening rondom grensoverschrijdende elektronische identificatie (EU 910/2014).

Verbetering DigiD

In 2014 getroffen maatregelen ter verbetering van (de betrouwbaarheid van) DigiD

– Bij ontdekking van zogeheten phishing-sites worden deze websites in samenwerking met de Belastingdienst en het Nationaal Cyber Security Centrum (NCSC) zo snel mogelijk uit de lucht gehaald. In 2014 zijn er ruim 40 sites op deze manier uit de lucht gehaald.
– Op de website van DigiD wordt door Logius advies gegeven over het veilig omgaan met DigiD. Daarbij wordt onder meer gewezen op het belang dat de gebruiker controleert dat hij/zij daadwerkelijk inlogt op de echte inlogpagina van DigiD. Ook wordt gewaarschuwd voor valse e-mails waarin wordt gevraagd om inloggegevens in te vullen. Bovendien wordt uitgelegd hoe de gebruiker misbruik van zijn account kan herkennen en welke actie hij kan ondernemen bij geconstateerd misbruik. Tenslotte wordt verwezen naar de ondersteuning die kan worden geboden onder meer via de helpdesk van DigiD, het Centraal Meldpunt Identiteitsfraude en het Meldpunt Slachtoffers Fraude van de Belastingdienst.
– In de brede Alert-Online-campagne is in 2014 aandacht besteed aan veilig internetten.
– Burgers kunnen er nu zelf ervoor kiezen om standaard in te loggen op niveau Midden. Dat maakt hen – vanwege de tweede authenticatie door middel van SMS – minder kwetsbaar voor bijvoorbeeld phishing.
– Inmiddels heeft 80% van de DigiD gebruikers een mobiel nummer ingevoerd. In 2014 was een stijging van 32,7% te zien op het gebruik van DigiD Midden ten opzichte van 2013. (Aantal transacties op niveau midden heel 2013: 9.128.861. Aantal transacties op niveau midden heel 2014: 12.116.611. Groei 2013 naar 2014: 2.987.750.)
– Er worden voortaan e-mails verstuurd aan burgers bij belangrijke wijzigingen aan hun DigiD, zoals bij het wijzigen van een wachtwoord. Op die manier wordt het makkelijker voor burgers om misbruik van hun DigiD te herkennen.
– DigiD activeringscodes worden in kwetsbare postcodegebieden thuisbezorgd. In totaal zijn in 2014 ca. 7.500 brieven thuisbezorgd per koerier.
– Er zijn maatregelen tegen DDoS-aanvallen genomen. Dit is belangrijk voor de beschikbaarheid en continuïteit van DigiD maar ook voor de veiligheid.
– DigiD is beveiligd om het mogelijk te maken beter de integriteit en authenticiteit van de website te controleren en phishing te bemoeilijken.

In 2015 te treffen maatregelen ter verbetering van (de betrouwbaarheid van) DigiD

Voor 2015 heb ik een versterkingsagenda opgesteld die een samenstel is van diverse extra acties die vanuit ICT en kostenperspectief de meest effectieve stappen zijn.

Alternatief DigiD Midden

In de eerste plaats wordt een alternatief voor het redelijk kostbare DigiD Midden met SMS gerealiseerd, dat tegen lagere kosten op grote schaal kan worden toegepast. In februari start de bouw van de beoogde oplossing, medio 2015 wordt de beoogde oplossing beproefd in een pilot. Mocht de pilot succesvol blijken, dan zal besloten worden over een brede uitrol.

Versterking DigiD met identiteitsdocument, niveau 3

Door enkele grote uitvoeringsinstanties worden in 2015 pilots uitgevoerd met het toepassen van een extra controle na het inloggen met DigiD. Die extra controle vindt plaats door het uitlezen van gegevens op de chip van een wettelijk identiteitsdocument, zoals de Nederlandse identiteitskaart en het rijbewijs. Daarmee wordt het mogelijk authenticaties met betrouwbaarheidsniveau STORK 3 uit te voeren. Mochten de pilots succesvol zijn, zal ik laten onderzoeken of deze methode overheidsbreed kan worden toegepast.

Publiek middel op hoogste betrouwbaarheidsniveau, niveau 4

Het kabinet acht het mogelijk en wenselijk in een publiek eID-middel te voorzien binnen het eID stelsel, waarmee authenticaties op het hoogste niveau mogelijk worden. Er worden momenteel voorbereidingen getroffen om kleinschalige pilots te starten met een publiek eID-middel.

ICT-Beveiligingsassessments DigiD

Tot slot worden alle DigiD-gebruikende organisaties geacht, vóór 1 mei 2015, hun jaarlijkse rapportages over hun ICT-beveiligingsassessment DigiD op te leveren.

eID Stelsel als toekomstige standaard

Het beleid van het kabinet is erop gericht om de dienstverlening door de overheid en het bedrijfsleven digitaal, veilig en toegankelijk te maken voor burgers en bedrijven. Om het vertrouwen in digitale dienstverlening te waarborgen, is het op betrouwbare wijze geven van toegang tot digitale diensten, nu en in de toekomst, van primair belang. In dat verband heeft de overheid in 2012 het initiatief genomen om de mogelijkheden van een stelsel van afspraken te onderzoeken en ontwikkelen (eID Stelsel), met daarbinnen ruimte voor zowel publieke als private elektronische authenticatiemiddelen (eID-middelen) zodat er, naast DigiD, meerdere middelen op alle betrouwbaarheidsniveaus beschikbaar kunnen komen voor burgers. Het kabinet wil dit afsprakenstelsel vorm geven in samenwerking tussen overheid en bedrijfsleven. De Tweede Kamer is hierover onder meer geïnformeerd bij brief van 19 december 2013.[3]

Het eID Stelsel gaat uit van een multimiddelenstrategie, waarin hoogwaardige eID-middelen naast elkaar functioneren. Dat kunnen zowel publieke als private middelen zijn. Voor de publieke sector betekent dit dat er een publieke authenticatiedienst moet komen.

Het grote voordeel van de multimiddelen-strategie is, dat bij uitval van een inlogmiddel, burgers een ander inlogmiddel kunnen gebruiken. Voor de publieke sector is dit zeer belangrijk. Zonder de multimiddelenstrategie kan een «single point of failure» het risico inhouden dat essentiële overheidsdienstverlening gedurende kortere of langere tijd niet bereikbaar is. Gezien het belang van de dienstverlening voor veel burgers is dat een onwenselijke situatie.

In de tweede helft van 2015 zal een aantal pilots worden uitgevoerd, waarbij aan burgers met private eID-middelen toegang kan worden verleend tot publieke dienstverleners. Aan private eID-middelen die op deze voorziening worden toegelaten zullen strikte eisen worden gesteld met betrekking tot veiligheid en betrouwbaarheid, alsmede privacya-

[3] Tweede Kamer, jaarvergadering 2014–2015, 26 643, nr. 299

specten die in acht genomen moeten worden. Ten aanzien van het definiëren van betrouwbaarheidsniveaus voor elektronische identificatie zijn de Europese afspraken die gemaakt worden in het kader van de Europese verordening (EU 910/2014) betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties, leidend.

In deze eerste fase van het eID stelsel kunnen op de hiervoor geschetste wijze private eID-middelen door burgers worden gebruikt bij dienstverlening in het publieke domein. In de komende periode wordt daarvoor een pilotplan opgesteld waarin is vastgelegd welke diensten daarbij worden betrokken. De Belastingdienst voert daarbij ook een verkenning uit voor de inzet van bankmiddelen in een pilot.

In 2014 is een aantal verkenningen afgerond waarvan de vastgestelde rapporten worden gepubliceerd op de website: www.eid-stelsel.nl.[4] De verkenningen bevestigen het kabinet in zijn keuze voor het eID Stelsel. De opvatting van het kabinet, dat vaart gemaakt moet worden, wordt breed gesteund. Daarbij zijn zorgvuldigheid en het realiseren van waarborgen belangrijke vereisten. Het kabinet geeft zich nadrukkelijk rekenschap van het feit, dat het ontwikkelen van het eID Stelsel een complexe opgave is, waarbij passende beheersmaatregelen moeten worden genomen. Daarbij gaat het onder meer om een strikte voortgangsbewaking en kwaliteitscontrole.

Voor het eID Stelsel is het doel om in 2015 een eerste versie werkend afsprakenstelsel in de vorm van een Introductieplateau eID te realiseren, zodat pilots kunnen worden uitgevoerd. Parallel aan de uitvoering van dit Introductieplateau eID zal samen met maatschappelijke organisaties een visie worden ontwikkeld voor een vervolg op het Introductieplateau eID. Deze visie kan dan worden vertaald in een nieuw plateau van het eID Stelsel dat in 2017 vorm moet hebben gekregen. In het Introductieplateau eID wordt het eID Stelsel uitgewerkt naar inhoud, governance, toezicht en financiën, binnen een passend juridisch kader. Het bestaande stelsel voor authenticatie voor bedrijven, eHerkenning, dienst als basis voor het Introductieplateau eID. Het afsprakenstelsel eHerkenning zal daarmee in de komende periode migreren naar het eID Stelsel.

Concreet wordt voorzien dat eind 2015 wordt begonnen met een eerste fase van het afsprakenstelsel eID. De inrichting van deze eerste fase is mede met private partijen uit het eID platform vormgegeven. In de eerste fase zal nadrukkelijk aandacht worden gegeven aan aspecten van veiligheid, betrouwbaarheid en privacy. Daarbij worden de best beschikbare technologieën als uitgangspunt genomen. Ook zal toezicht worden ingericht om te borgen dat deelnemers aan het stelsel vertrouwd kunnen worden en veilig werken.

Op basis van de ervaringen met deze eerste fase van het afsprakenstelsel zal in de loop van 2016 worden bepaald of en op welke wijze aanvullende maatregelen of voorzieningen in het afsprakenstelsel opgenomen dienen te worden. Ook kan hierna een nieuwe functionaliteit in het stelsel worden opgenomen.

---

[4] Rapporten:
– Advies over het gebruik van publieke middelen in het eID stelsel, ECP 07-01-2015;
– Business Case publieke eID-middelen (integrale business case), Ecorys, 02-12-2014;
– Publieksonderzoek elektronische identiteitskaart, Motivaction, 26-09-2014;
– Internationale vergelijking eID-middelen, PBLQ HEC, 21-10-2014.

Ik vertrouw erop dat ik met deze informatie voldoe aan de door mij gedane toezegging.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk